UNITED STATES DISTRICT COURT

NORTHERN DISTRICT OF CALIFORNIA

OAKLAND DIVISION

EPIC GAMES, INC.,

Plaintiff, Counter-defendant,

vs.

APPLE INC.,

Defendant, Counterclaimant.

No. 4:20-CV-05640-YGR-TSH

WRITTEN DIRECT TESTIMONY OF AVIEL D. RUBIN, PH.D.

Trial Date: May 3, 2021
Time: 8:00 a.m.
Courtroom: 1, 4th Floor
Judge: Hon. Yvonne Gonzalez Rogers

Ex. Exhibit 11

I. Summary of Opinions

1. My analysis in this matter focuses on the security, privacy, and reliability of iOS, and particularly the question of whether Apple's App Review process and App Store distribution of apps provide and enhance the security, privacy, and reliability of iOS. It is my overall conclusion that Apple's App Review and App Store distribution provide significant security benefits that meaningfully contribute to iOS being a safer and more trustworthy platform than others. Allowing alternative app stores for iOS would prevent or weaken Apple's App Review and App Store distribution protections and would, in turn, weaken iOS and open it to new threats. This overall conclusion is based on the following opinions:

2. **Opinion 1.** Security for computing devices includes detecting and preventing malware. But it encompasses additional considerations such as ensuring user privacy, preventing scams, ensuring device reliability, and protecting developers and consumers from software piracy. (¶¶ 16-28.)

3. **Opinion 2.** Security assessments must consider the threat model, which is an analysis of factors including who wants to attack the device / user, how frequently such attacks are likely to occur, and what the consequences are (for the attacker and the victim) of a successful attack. With over 1 billion active devices that are almost constantly on and connected to the Internet, a userbase that frequently downloads apps and engages in financial transaction on the device, and camera, microphone, and GPS hardware that follows owners nearly everywhere they go, and nearly two million apps available for download, iOS—and Apple iOS devices such as the iPhone—are faced with an extraordinary threat model. The portability of these devices has facilitated their use for critical tasks such as navigation and emergency calls, but also means that they are at higher risk of being misplaced or stolen, which places the contents of that device at even greater risk. (¶¶ 22-28.)

4. **Opinion 3.** Computing security best practices call for layered defenses. This means that there are multiple defenses in place for each of the multiple types of threats that the device is likely to face. iOS layers defenses by combining on-device protections, such as access controls to limit the exposure of data and functionality, with additional review or verification mechanisms. Each layer of protection strengthens the overall security posture of the system, by lowering the risk that untrustworthy or malicious apps may reach an iOS device and reducing the impact of such apps should they make it to the device. (¶¶ 22-43.)

5. **Opinion 4.** Apple's App Review (and accompanying app distribution model) is one of the defense layers that Apple has employed to protect iOS devices and users. Using a combination of human reviewers and sophisticated computer analytical tools, the App Review provides significant security and non-security benefits by screening apps for a variety of potential problems including scams, privacy intrusions, piracy, objectionable content, as well as problems with reliability and crashing. By positioning itself as the sole source of app distribution, Apple prevents users from unintentionally or unknowingly downloading apps that would have failed the App Review process, and also prevents apps that fail the App Review process from simply relocating to another store with lower (or no) standards. (¶¶ 25-43, 53-76.)

6. **Opinion 5.** The App Review process, combined with other protective layers employed by Apple, has resulted in iOS being safer than other platforms, facing fewer attacks and malware infections than other platforms. Studies have found that Android devices are fifty times more likely to be infected with malware when compared to iOS, made up 26.64% of infected devices in 2020 (as opposed to iPhones, which accounted for only 1.72% of infected devices), and saw three times as many reported Common Vulnerabilities and Exposures ("CVEs") as Apple, with Android amassing 2,395 CVEs and iOS 832 CVEs between 2016-2019. Apple has achieved this result in spite of the extraordinary threat model that iOS device faces. (¶¶ 44-61.)

7. ~~**Opinion 6.** The introduction of alternative app stores on iOS devices would jeopardize the security, safety, and trustworthiness of the iOS platform. Many other distribution sources simply will not prioritize security, safety, and trustworthiness. We know this because outside of the iOS platform, there exist stores that primarily traffic in adult content, malware, and/or pirated software. Even distribution sources that mean well would have trouble meeting the standards of Apple's App Review. Some of them will lack the resources to build the various tools and employ the reviewers that Apple currently has on staff. Others will lack the incentives. For example, developers and third-party stores whose financial model depends largely on ad revenues will have less incentive to protect user privacy because much of ad revenue is based on the ability of advertisers to target and know intimate details about end users. And finally, all other sources will lack Apple's knowledge of iOS and iPhone hardware and their security vulnerabilities, as well as the extensive body of knowledge that Apple has accumulated from more than a decade of app review and analysis of threats posed by apps. Internal knowledge of iOS and iPhone architecture cannot be simply revealed to third parties because of the potential associated security threats. (¶¶ 77-117.)~~

8. **Opinion 7.** Fragmentation of app distribution and review would undermine security. Security is only as strong as its weakest link; where multiple app stores are available, a bad actor could seek out the option that is least likely to protect against malicious or otherwise problematic apps. And Apple's App Review benefits from its ability and knowledge gained from holistic review across its platform. (¶¶ 87-99.)

9. **Opinion 8.** The current Android marketplace in China demonstrate the problems with fragmentation. In China, where Google's Play Store is banned, numerous third-party app stores operate in its stead. Google has little control over the various Android app stores, which are known to host a higher prevalence of fake, cloned, and malicious apps than the Google Play store for which Google conducts app review. In fact, China hosts the top three stores from which users are most likely to download malware—Xiaomi, Baidu, and Pconline—and more generally, nearly 35 percent of Android apps were found to secretly steal user data unrelated to the app's functionality. The multitude of app stores in China has thus led to generally looser security standards, numerous stores that violate security and privacy regulations, and, consequently, a proliferation of malicious apps in China's Android market. (¶¶ 100-04.)

10. **Opinion 9.** Changing iOS likely would open new threats and negative security impacts. In particular, it would entail changing security measures that Epic's experts have identified as significant and important. Epic's experts propose a hypothetical world with significant negative security impacts that they have not fully assessed. (¶¶ 105-24.)

11. **Opinion 10.** Diversifying In-App Purchase ("IAP") channels would inhibit Apple's anti-fraud abilities. The App Store's requirement for use of IAP enhances user security, including by use of Apple's cryptographic hardware. (¶¶ 125-29.)

II. Background and Qualifications

12. I have 30 years of experience in the field of computer science, and specifically in Internet and computer security.

13. I received my Ph.D. in Computer Science and Engineering from the University of Michigan, Ann Arbor, in 1994, with a specialty in computer security and cryptographic protocols. I have been Professor of Computer Science at Johns Hopkins University since 2003. I am also the Technical Director of the Johns Hopkins University Information Security Institute—the University's focal point for research and education in information security, assurance, and privacy. Johns Hopkins University, through the Information Security Institute's leadership, has been designated as a Center of Academic Excellence in Information Assurance by the National Security Agency and leading experts in the field.

14. I also have significant industry experience. I spent six years at AT&T Labs in the Secure Systems Research Department, where I focused on Internet and computer security. Prior to AT&T Labs, I spent two years at Bellcore in its Cryptography and Network Security Research group, also focusing on Internet and computer security issues. More recently, I served as the founder and President of Independent Security Evaluators, a computer security consulting firm. Among our responsibilities was acting as an independent testing lab for Consumer Union, which produces the Consumer Reports magazine. For Consumer Union, I managed an annual project where we tested popular anti-virus projects. I am also currently the founder and chief scientist of Harbor Labs, a software and networking consulting firm specializing in medical device security and privacy of healthcare data.

15. I serve, or have served, on several technical and editorial advisory boards. I have served on the Editorial and Advisory Board for the International Journal of Information and Computer Security, the Journal of Privacy Technology, and Springer's Information Security and Cryptographic Book Series, as well as acting as an Associate Editor of the Institute of Electrical and Electronics Engineers' ("IEEE") Security and Privacy Magazine, the Association for Computing Machinery's ("ACM") Transactions on Internet Technology, and the Communications of the ACM journal. I also have served in the past as a member of the Defense Advanced Research Projects Agency's Information Science and Technology Study Group, a member of the Government Infosec Science and Technology Study Group of Malicious Code, Associate Editor of the Electronic Commerce Research Journal, Co-editor of the Electronic Newsletter of the IEEE Technical Committee on Security and Privacy, and a member of the board of directors of the USENIX Association (the leading academic computing systems society).

III. Opinions

A. Security Encompasses Broad Categories and Must Consider the Threat Model

1. Security Encompasses Safety, Privacy, Trustworthiness, Piracy, Objectionable Content, and Reliability

16. While the definition will vary depending on the context, **security** generally refers to the process of protecting data as well as device and system functionality.

17. For purposes of my opinions in this case, I take a broader view of security than Epic's experts, Dr. Lee and Dr. Mickens. In particular, Drs. Lee and Mickens appear to be almost exclusively focused on the narrow goals of malware exclusion and exploit resistance. Malware is typically defined as software designed to disrupt, damage, or gain unauthorized access to a system. Exploit resistance generally refers to a system's ability to enforce the security measures in place (e.g., preventing users who do not have a password from accessing a password-protected system). With this narrow focus, Drs. Lee and Mickens conclude that certain of Apple's App Review goals do not relate to security because they instead relate to broader subjects such as safety, performance, business, design, and legal compliance.

18. I agree that malware exclusion and exploit resistance are important security goals. But I take the broader view that security encompasses issues including **privacy**, **trustworthiness,** and **reliability.** For example, if an app is targeted to young children, and asks the user to enter her age and home address, that is a potential security concern. If an app says that it is a program that allows a user to play Tic-Tac-Toe against the device, but wants to access the device's microphone and camera for reasons entirely unrelated to Tic-Tac-Toe, that is a potential security concern. If an app developer scams users by falsely describing the application as one that can detect a stroke, or by artificially inflating an app's reviews to entice customers to purchase the app, those also are potential security concerns. Privacy relates to protecting data from unauthorized access or disclosure, and is intertwined with security: security and privacy are two sides of the same coin, where security controls dictate the level of privacy enforced, and privacy technologies can guarantee a higher degree of security.

19. Unreliable apps also expand the attack surface, or different points of entry by which security can be attacked. If an application is supposed to remind a user to take medication at a certain time, but constantly crashes and fails to do that, that is a potential security concern. As this and the earlier examples demonstrate, apps are more and more frequently used in the management of daily life and home, and unsafe or unreliable apps could have physical security implications. Reliability and security are intertwined, because reliability ensures that security controls work as expected. Decreases in security and reliability thus likely coincide. For example, a software crash could indicate that a threat has been embedded in an app's code or otherwise create an opening for an attacker to take advantage of the cause of that crash to, for example, transmit a custom input that redirects the app to a location containing a virus or other malware.

20. Reviewing for legal compliance likewise aids in protecting security. **Piracy**, for example, is a security risk, not just a content moderation issue. Pirated apps threaten users because they are known to often contain malicious functionality. And pirated apps threaten developers because the download of pirated apps reduces the revenue stream for the legitimate version of those apps. Other illegal apps pose similar threats. Apps that, for example, enable illegal gambling could exploit user information or wealth.

21. For similar reasons, reviewing for **objectionable content** can contribute to security. Drs. Lee and Mickens had identified "objectionable content" review as "non-security concerns." But objectionable content such as pornography is frequently associated with malware. Kaspersky, a global cybersecurity company that provides antivirus and other cybersecurity products, found that over 25% of attacks on mobile devices come from porn-related malware. This arises in part because apps and sites distributing pornography have fewer traditional revenue mechanisms available to them, and thus have been found to be more likely to partner with malicious actors in their efforts to monetize their sites. All of these examples illustrate the broader point that security is not limited to just anti-virus scanning and exploit resistance mechanisms.

2. iOS Faces a Heightened Threat Model

22. Any evaluation of the security of iOS thus must consider its context, objectives, potential attackers, and the manner in which users use their systems, or the iOS "threat model." Threat models help formalize the security risks to a system, by enumerating vulnerabilities, weaknesses, and defects, as well as impact of their exploitation. For example, it is important to ask: What might a potential attacker be motivated to attack, and why? What data could be targeted by the attacker? Would an attack require sophisticated hardware? What mechanisms could the attacker use in seeking to recover private data from an iPhone? How physically accessible is an iPhone, and the data that it contains? How many users could be impacted? What would the potential cost of an attack be?

23. With over 1 billion active devices, an App Store that hosts almost 2 million apps that have been downloaded over 180 billion times, a user base that frequently downloads apps and engages in financial transactions on the device, and camera, microphone, and GPS hardware that follows users nearly everywhere they go, Apple iOS devices are faced with an extraordinary threat model. iOS devices are small, portable, typically on 24/7 and kept close at hand by users for critical tasks such as navigation and emergency calls. They are very likely to hold a user's financial information, personally identifiable information ("PII"), protected health information ("PHI"), and location information. And they might be misplaced, lost, or stolen at a higher frequency than other types of computer systems. Their convenience has led users to store more private information on them, and users rely on their functionality. All of these reasons, however, make iOS devices rewarding targets to attackers and thus heighten the risks they face.

24. A factor in the threat model is the sophistication of potential attackers. Malware developers and other malicious actors continue to become more sophisticated and expend significant resources to build malicious and other ill-intentioned apps for mobile devices. Purplesec, a cybersecurity company, observed in DX-4956, a report published in 2020, that the total malware infection growth rate has been increasing by hundreds of millions every year

(812.67 million infections reported in 2018, a significant increase from 702.06 million reported in 2017). Among the better-resourced are Advanced Persistent Threat ("APT") groups, which are usually directed and supported by established nation-states to conduct cyberattacks on government, industry, and infrastructure targets for political or economic agendas. APT groups use malicious apps to target high-profile victims and cause long-term damage on critical assets through, for example, spyware that collects recordings, locations, messages, and call logs from infected users. Social engineering attacks also are on the rise—they were observed as comprising 98% of cyber-attacks in 2020. Social engineering attacks are exploit problems designed to manipulate users into taking actions that will disable or circumvent existing on-device or other affirmative protections. Cybersecurity cannot be static, because malicious actors are always seeking out new vulnerabilities in systems and ways to circumvent and evade anti-malware and other security mechanisms.

25. In view of the wide variety of potential attacks, and the mechanisms they can use, computing security best practices calls for the employment of layered defenses. This is true for iOS and more generally. The concept of layered defenses is based on the understanding that the more layers of protection that a system has, the harder the system is to exploit. Each additional layer of protection enhances the overall security posture of the overall system. In computer systems generally, and in iOS in particular, layered security combines access controls to limit the exposure of data and functionality as well as additional security review or verification mechanisms. By doing so, there is lowered risk of unwanted apps ever reaching an iOS device and users being confronted with social engineering attacks, as well as reduced impact of unwanted apps should they be able to make to the device.

26. Take the example of a Tic-Tac-Toe app that I mentioned earlier, where the Tic-Tac-Toe app would access an iPhone's microphone and camera. That app, on its face, may not be sufficiently limited by access controls, because there may be a legitimate reason why users playing Tic-Tac-Toe may want to talk to each other. However, additional security review and verification mechanisms, such as Apple's App Review process, are better positioned to evaluate not just that there is microphone and camera access, but whether that microphone and camera access has malicious ulterior motives. And the microphone and camera are not the only hardware on an iOS device that could expose a user. Even an iPhone's Bluetooth functionality, for example, can be used to determine its user's location—thereby potentially putting the user's safety and privacy at risk—if an app is permitted to poll for nearby Bluetooth devices. A thief, for example, could develop an app that would use this Bluetooth capability to provide an alert anytime a user was (a) far enough away from their home that the house was vulnerable to burglary or (b) in a particular location and personally vulnerable to attack or pick-pocketing. For this reason, Apple scrutinizes requests to use Bluetooth functionality without a legitimate reason.

27. Apple has implemented sandboxing and other on-device protections, as well as taken additional measures to enforce user privacy by, for example, requiring users to opt in before sharing data and implementing differential privacy techniques that de-individuates user data. Social engineering attacks, however, are designed to manipulate users into taking actions that avoid these protections. For example, consider a game app that, while being run, will instruct a user to enter their social security number to proceed to the next level. Here, all the app did was display some text content. That would be unlikely to trigger any of the security properties that

Dr. Mickens identifies as providing sufficient security for iOS but likely would, as I will explain, be detected during App Review.

28. Another example of a social engineering attack is presented by the "Update your Adobe Flash plugin" pop-up scam, where multiple malicious websites relied upon general familiarity with the "Adobe Flash Player" program to disguise malware in a pop-up advertised as an Adobe Flash Player update. Users who thought they were agreeing to update their Flash Player were instead deliberately installing adware (malware that would hide on their device, show unwanted advertisements, and/or track user behavior) or worse. Scams and phishing campaigns do not directly subvert on-device security measures, but instead exploit the (misplaced) trust between the user and the vehicle through which a user would download the app.

B. Apple's App Review Provides Significant and Better Security and Non-Security Benefits than Competitor Platforms

29. Apple recognized the importance of layered security in designing its security architecture to meet dual goals. First, the App Review and app distribution process seeks to prevent unsafe apps from ever reaching user devices in the first place if threats and vulnerabilities are detected. Second, Apple's on-device security seeks to protect against and limit any damage that can be inflicted by an app that is installed on a device.

30. It is generally unwise to *first* trust users to download malicious apps, and *then* try to subsequently detect malicious apps and deny giving malicious apps the permissions they might request. Given the unpredictability of user behaviors that may lead to vulnerabilities and exploitations, users might still keep or run a malware even though an anti-malware identifies it, or send the piece of malware to other users without running it. It is better to prevent user devices from ever being infected with malware—as Apple endeavors to do with iOS—rather than use on-device solutions to attempt to identify and remove malware once it already resides on a device.

31. Apple's App Review security layer is a necessary complement to on-device protections such as sandboxing to prevent apps from accessing data and functionality that they should not be permitted to access: App Review checks an app to make sure it is not requesting unnecessary entitlements (or special access rights to other hardware or software on an iOS device), which is often an indication of malicious behavior. Sandboxing then enforces these entitlements, only allowing apps access to data and functionality that the user permits the app to have. Sandboxing also prevents apps from accessing and modifying data that is written by other apps.

32. Apple's use of the App Store as the single app distribution mechanism adds a protective layer for iOS devices. Apple currently conducts review on every app and app update distributed through the App Store using a combination of computer automated and manual human review. By centralizing the distribution of apps and prohibiting the distribution of apps outside of the App Store, Apple forces any would-be attacker to navigate this additional layer of defense. Without exclusive app distribution, apps could bypass the App Review layer of defense.

33. Apple's app distribution layer provides additional protections even if App Review does not catch a breach in the first instance. Where apps are all distributed through the App Store, if an untrustworthy or malicious app is identified, Apple can pull this app (as well as other similar

ones) from the App Store to stop further distribution, or, as Steve Jobs put it, "turn off the spigot" so no more people can download that app (or similar ones).

34. Permitting alternative third-party app stores would increase instabilities and security risks for iOS. As I'll explain, alternative platforms that permit apps to be downloaded outside a reviewed distribution channel have demonstrably greater security vulnerabilities and concerns. Also instructive are the limited scenarios in which Apple permits apps to be downloaded outside of the App Store; Apple has observed efforts to take advantage of those scenarios to circumvent security requirements.

35. Epic and its experts characterize Apple's App Review process as generally ineffective, easily replicable by third parties, and providing minimal security benefits beyond what on-device security mechanisms already provide. As noted above, they reach this conclusion based on a narrow definition of what constitutes a security risk. And in any event, none of these criticisms are true. Apple's App Review constitutes a critical component of Apple's layered security that provides significant and effective security protections that enhance and improve the security of iOS.

1. Apple's App Review Process Provides Significant and Comprehensive Security Protections That Complement On-Device Protections in Providing a Safe and Trustworthy iOS Platform

36. Apple's App Review is necessary to complement Apple's iOS on-device security in protecting against malicious apps. App Review, and particularly its review by humans of every app and app update approved for distribution through the App Store, provides comprehensive advantages in identifying and mitigating malicious and untrustworthy activities within an app. In other words, conducting App Review means that iOS apps are more likely to function as disclosed to users and are less likely to contain malware, undisclosed and unintended features, and other unsafe features. For the examples I provided earlier, and for other types of untrustworthy or malicious apps, on-device security alone would not provide sufficient protection.

37. App Review is better positioned than on-device security mechanisms to evaluate user-generated content and determine whether entitlement access is being requested for a legitimate or ulterior motive. Apple's App Review, for example, is better able to detect social engineering attacks like a game app that instructs users to enter private information like their social security numbers. App Review also is better able to flag the Tic-Tac-Toe app that will act as spyware via its access to an iPhone's microphone and camera. A software running on the device will not find it suspicious that a Tic-Tac-Toe app should want access to the microphone and camera. App Review is better positioned than on-device security mechanisms to detect and prevent adware. App Review also is better positioned to determine whether an app contains hidden and undisclosed behavior, or will do everything it promises to do. It is difficult for a machine to know whether an app purportedly about renaissance art actually contains such content.

38. The human review component of Apple's App Review is critical; its combination with the static and dynamic analysis performed by Apple's proprietary computer systems differentiates and strengthens iOS security. Human reviewers are better able than computers to

accurately assess, for example, whether user-generated content is offensive, violates restrictions on content in apps for children, constitutes false or misleading content, or seeks information in violation of privacy guidelines. Human review also is critical in light of the "halting problem" faced by computer tools, where it is difficult for computer programs to determine when earlier programs will "halt," or terminate. Apps are comprised of multiple computer programs, where each program will be "called" to run in turn. But the next-in-line program does not know when it will begin to operate until it is called; that program is not, unlike a human, able to take a global look at the overall app architecture or predict future behavior. For this reason, computer tools may have a more difficult time determining whether an app has hidden a problematic feature in a program, especially when the malicious components had not been previously identified. For example, in the game app I mentioned earlier, users were instructed to enter their social security number in a malicious game app. If the malicious component is novel or obfuscated and hidden in a certain way, App Review computer tools or on-device protections might not detect it. By contrast, human reviewers might detect the issue because they would see the text content as part of the app's overall media content.

39. Humans are also better equipped to evaluate the motivations for an app that instructs its users to actively restart their device or disable device security features, which, in turn, could expose users to uncontrolled or untrusted apps and code or permit a device to run undisclosed operations in the background. An example of this type of threat is cryptojacking malware, or malware that harnesses its compromised device's resources to run background operations that mine cryptocurrency. The question of whether cryptomining is authorized can be context-dependent, which makes it difficult for traditional anti-malware to determine whether an app mining cryptocurrency is doing so with the user's consent and knowledge, or as a result of cryptojacking. Absent Apple's App Review process, it would be up to the users to decide whether to grant potentially malicious apps access to the camera, network, microphone, etc. or decide whether to disable certain on-device security features that the app claims will affect its operation. App Review is critical to maintaining the users' sense of trust and preventing users from having to make difficult cybersecurity-based decisions.

40. App review's human review component also means that it is better positioned than on-device mechanisms to detect new types of issues and threats. Computer tools rely upon heuristics—or algorithms that are written by humans to define patterns or other indicia of potentially unsafe activity—but are also fundamentally limited by that reliance. Heuristics are well-suited for identifying already-known threats and performing repetitive analysis, but are less able to detect something that was not previously known and therefore not addressed in the existing algorithms.

41. Apple's App Review process benefits from a significant number of resources that enhance its accuracy and efficiency. First, App Review process benefits from its proprietary machine learning and other computer tools that it has developed for the app review process. Apple has committed to and invested heavily in the development of these tools, which are used internally by Apple and are not available to third-party reviewers.

42. Second, Apple's App Review process benefits from the information that is has garnered through over a decade of app review. Such accumulated information—all of which is held as proprietary—includes a large internal corpus of previously identified threats associated with

rejected malicious apps, including suspicious keywords, malicious IP addresses and URLs, and information used to determine whether an app may be pirated. This information, which is developed in connection with the human review that Apple conducts of every app and app update approved for distribution through the App Store and Apple's underlying knowledge of the iOS ecosystem, has multiple purposes. Apple utilizes this data to train its machine learning algorithms to better detect malicious and otherwise problematic apps. Apple also utilizes this information internally to improve iOS security.

43. Third, Apple's knowledge of its own iOS ecosystem and operation and their security vulnerabilities, as well as its private APIs, plays a critical role in Apple's App Review. Apple's internal knowledge of the detailed operation of iOS, its potential vulnerabilities and development, private APIs, and first-party entitlements are highly associated with security concerns. APIs, for example, are interfaces through which an app can access system functions. Apple has created a list of private APIs and determined that they should be used by Apple only for its internal purposes. Such information, if subverted, can grant bad actors heightened privileges to perform powerful security attacks on iOS devices. For these reasons, disclosure of confidential and proprietary information about iOS and iPhone hardware can create significant security risks. Restricting third-party developers' access to Apple's private APIs helps ensure that apps cannot interfere with the core functions and stability of iOS.

2. iOS Is Safer than Other Operating System Platforms

44. I disagree with the conclusion of Drs. Lee and Mickens that other platforms, such as Windows and Android, offer "rough parity" in their security protections to those of iOS. A number of objective third-party sources indicate that iOS is safer. These third-party sources reinforce my own conclusion that the particular attributes of Apple's App Review render iOS a safer and more trustworthy platform.

a) Third-Party Analyses Demonstrate that iOS Is Safer than Other Platforms

45. Non-iOS mobile devices historically have been the victims of malware far more often than iOS devices. For example, the National Vulnerability Database ("NVD"), maintained by the National Institute of Standards and Technology ("NIST"), collects Common Vulnerabilities and Exposures ("CVEs") reported for various software platforms. A CVE is a broad term that refers to computer security flaws and includes, for example, authorization bypass efforts, reliability problems such as buffer overflows, the exposure of sensitive information to unauthorized actors, improper privilege management, and other flaws in software, hardware, or computer components that can be exploited and negatively impact confidentiality, integrity, or the availability of that component. The NVD's CVEs are considered by the industry to provide indicia of a platform's relative security or trustworthiness because they provide a standardized identifier for given security flaws and enables the assessment of information across multiple platforms. The NVD acts as the U.S. government repository of standards-based vulnerability management data and is recognized by the industry as a leading source of software vulnerability data. As shown in DX-4962, DX-4969, and DX-4966, the chart below reflects the number of CVEs on iOS compared to the numbers on Android and Debian Linux operating systems in

recent years. In each year, iOS had only a fraction of the number of CVEs that Android and Debian Linux had.

Year	Number of CVE Entries		
	iOS	Android	Debian Linux
2016	164	525	336
2017	387	843	456
2018	125	613	1200
2019	156	414	360

46. By comparison, Android has been reported to have the most vulnerabilities for three out of the four years from 2016-2019 by NVD, and is consistently found to be more affected by malware than iOS. DX-4959, a 2019 cybersecurity report, showed that Android devices are "fifty times more likely to be infected with malware when compared to iOS."

47. Similarly, DX-4975, a study conducted by Nokia in 2020, found that 26.64% of infected devices ran an Android-based mobile operating system. These statistics stand in comparison to those for iPhone, which accounted for only 1.72% of infected devices in 2020. And DX-4975.008 attributes the greater percentage of Android infected devices to the fact that it permits the distribution of apps through third-party stores.

48. DX-4956, a Purplesec analysis, reports that 98% of mobile malware target Android devices, while DX-4959, a cybersecurity study conducted by Panda Security in 2019 showed that Android devices are "fifty times more likely to be infected with malware when compared to iOS." Additionally, DX-4975, a study done by Nokia shows that, in 2020, 26.64% of infected devices ran an Android-based mobile operating system. In comparison, iPhones accounted for 1.72% of infected devices. Nokia attributed this difference to Android devices permitting third-party app stores to distribute apps. In contrast to the centralized app distribution for iPhones, Android users can download apps from a variety of app stores: the Google Play Store overseen by Google, app stores developed by the original equipment manufacturers ("OEMs") of the various Android devices (such as the Samsung Galaxy Store), and app stores operated by various third parties unaffiliated with Google or Android device OEMs. The degree to which pre-distribution app review is performed by these various app stores varies. Nokia observed: "[T]he fact that Android applications can be downloaded from just about anywhere still represents a huge problem, as users are free to download apps from third-party app stores, where many of the applications, while functional, are Trojanized."

49. In fact, Android and third-party app stores have been found to host blacklisted apps with significantly greater frequency than the App Store. Blacklisted apps are apps identified as embedding potential security threats. Blacklisted apps include malware, adware, phishing apps that look like legitimate brands, and apps that perform suspicious activities such as overcharging users through fraudulent trials. DX-4401, a 2019 study by RiskIQ, identified the Google Play Store as the second most prolific store of blacklisted apps in 2019, hosting 25,647 malicious apps—less than half of the most prolific store, 9Game.com, which had 61,669 apps, but more than 5 times as many as the sixth most prolific source for blacklisted apps, wwwdownloadatoz. The App Store, although the fifth most prolific store of newly observed apps in 2019, was described as rarely hosting dangerous apps. In general, iOS consistently scores higher than

Android on metrics of perceived platform quality and user satisfaction because of Apple's diligence in ensuring app quality.

50. The Windows/PC platform also faces more vulnerabilities than iOS. In Nokia's study, Windows/PC devices accounted for an even higher percentage of infected devices than Android, at 38.92% in 2020. And Windows has a history of being victim to very damaging malware attacks. In 2017, for example, the NotPetya ransomware caused an estimated $10 billion in damages and disrupted the global supply chain by decommissioning a significant percentage of shipping ports employed by a certain shipping entity.

51. Throughout the App Store's existence, there have been incidences of new malware finding its way onto the App Store. Examples like these have been used by Epic and its experts to suggest that Apple's App Review fails to provide meaningful protections to users. Simply put, these cases do not show the lack of necessity for the App Review process. The third-party analyses that I just discussed, as well as Apple's internal statistics recording how many apps are rejected or otherwise taken down because of privacy violations, the introduction of hidden features, and obfuscation techniques (over 150,000 for privacy violations alone in 2020), among others, show how distorted Epic's experts' claims are. RiskIQ recognized that Apple's App Store is one of the fastest growing app stores, with 465,676 new apps observed in 2019, but described it as "Fort Knox…. [because] it rarely hosts dangerous apps." And, more generally, the App Store hosts almost 2 million apps that have been downloaded approximately 180 billion times, collectively. Apple reviews approximately 100,000 App Store submissions per week, which annualizes to more than five million apps and app updates per year. Even if 100 bad apps made it through the App Review process and became available on the App Store, that would still be less than 0.01 percent of the apps on the App Store and an even smaller percentage of the apps and app updates reviewed by App Review. And, importantly, Apple's App Review process is ongoing—it will continue to monitor and take down apps that are already available in the App Store, if it determines those apps are untrustworthy or malicious, and it modifies its App Review process when it learns of such apps to prevent similar apps from getting through App Review in the future. This evidences the relentlessness of threats and danger of degrading security.

52. For similar reasons, marketplace payout levels for "zero day vulnerabilities" are not instructive in evaluating whether Apple's App Review provides security benefits (or better or worse security benefits than those offered on Android devices). According to Dr. Mickens, the higher payouts offered for Android by Zerodium, one zero-day acquisition firm, demonstrate that iOS phones are easier to compromise than Android phones. But as Dr. Mickens himself admits, market data must be interpreted with a degree of skepticism. There can be many reasons for the varying levels of iOS and Android payouts including, as Dr. Mickens notes, the possibility that demand for iOS exploits is now depressed by the fact that the bounties for iOS vulnerabilities used to be higher than those for Android. Also possible is that Zerodium may offer a higher payout for Android because of Android's adaptability to various types of infrastructure and hardware (while iOS is intended for Apple devices only). I note as well that there are multiple zero-day acquisition firms, including government organizations and hacker groups operating in less visible, less trackable marketplaces, that offer different (and higher) payouts for iOS than Android. The amount of a payout simply cannot be assumed to directly correlate with level of security offered on a platform.

b) Apple's App Review Renders iOS a Safer and More Trustworthy Platform

53. The results of these third-party studies are consistent with and reinforce my conclusion that the iOS's layered defenses, and particularly its inclusion of the App Review layer, make iOS a safer and less vulnerable platform than competitor platforms. Windows, Android, and non-Android variants of Linux (shortened as "Linux") have much more lenient app distribution models, and depend on on-device security and third-party anti-malware solutions to then find solutions for the malware once it is already on device.

54. The Google Play Store, and the Android mobile platform more generally, provide a particularly instructive comparison because they permit multiple ways to circumvent any app review like Apple's App Review process. Unlike iOS, Android permits the installation of apps from multiple sources, including third-party stores, sideloading, and preloading by OEMs. Android also maintains fewer authorization mechanisms; it does not, for example, require apps to be signed with certificates obtained from Google or another principal authority. Android's official documentation recognizes third-party stores and sideloading as legitimate "[a]lternative distribution options." As such, the developer identity associated with sideloaded apps are not checked so that there is no deterrence for malicious Android app distribution via sideloading. Sideloading introduces security risks to users: it allows the installation of unreviewed apps that might install malware or otherwise might grant themselves entitlements to a broad array of hardware and software in order to, for example, access privileged functionality without alerting the user. These unreviewed apps also could be pirated or otherwise entail intellectual property violations. Additional security risks are posed because it is almost impossible to effectively limit further distribution of an already-identified malicious or vulnerable app, which can be downloaded through such a wide variety of means. It also is difficult to keep sideloaded apps up-to-date and secure.

55. These design choices stand in stark contrast to Apple's App Review and centralized app distribution security layers and, as I just explained, lead to significantly higher infections and other vulnerabilities in Android than in iOS. Apps that are sideloaded onto an Android device may undergo no app review at all and, for this reason, could contain any manner of malware or spyware. This happened in 2019, for example, when spyware was distributed through sideloaded Android apps that advertised themselves as Evernote, Google Play, and other massively popular apps, but instead were "fake apps" that performed eavesdropping, screen recording, and password collection from user devices.

56. The presence of third-party app stores containing unreviewed apps thus has the potential to significantly diminish the overall security of a platform. And this applies not just to pre-distribution app review, but also to apps after they become available for distribution in a store. Apple continues its App Review process even after an app becomes available for distribution in the App Store and will take action against apps that exhibit malicious or user-unfriendly behaviors after they have become available in the App Store. Apple is able to do all of these things because of its App Review and control of all aspects of its platform. Android, however, does not and cannot. iOS's ban on the installation of unsigned, untrusted apps enhances iOS security relative to Android.

57. It is not just the use of any app review, moreover, that makes iOS safer. It is also the specific process used by Apple in its App Review. Even where Google performs app review, as it does for the Google Play Store, the differences between Google's review and Apple's App Review demonstrate why Apple's human review component is particularly designed to protect against safety and trustworthiness threats. Google introduced human review into its previously entirely automated review, but only for some, not all, apps submitted to the Google Play Store in 2015, and [redacted]. Unlike Apple's App Review process, which performs human review for every app and app update approved for distribution through the App Store, [redacted]. Internal Google documents show, however, that Google acknowledges that its human-based review may not be as robust as others'. Google stated, for example, that it understands that "lots of bad stuff gets through" its review process. DX-4909.027. An internal Google presentation given in January 2019 stated that Google's review process [redacted] DX-3913.037. Additionally, [redacted] DX-3913.037. [redacted] DX-3913.037. The Google Play Store, which utilizes a less stringent and less comprehensive review process, stands in contrast to those for the App Store described as "Fort Knox."

58. This manifests in multiple examples of malicious apps found on the Google Play Store that would have been rejected in the App Store review process. One such example is AK Blackjack, a blackjack game that also runs clickfraud malware to, without user intent, create fraudulent ad revenue by contacting various ad-hosting websites. DX-3332.015. The AK Blackjack app utilizes a programming tool called Multidex to obfuscate its binary code. As I mentioned earlier, hidden features in obfuscated code are less easily detected by computer automated tools and, for this reason, is the focus of review by humans in Apple's App Review process and thus likely would have been detected by Apple. Apple's combination of human review with static and dynamic computer review that uses Apple's proprietary tools, for every app and app update distributed through the App Store, uniquely differentiates Apple's industry-leading process.

59. iOS's security advantage also can be directly attributed to the guidelines for Apple's App Review, which enhance security and promote a high-quality experience for the user. Although Google is gradually adopting more restrictive security policies similar to those in Apple's App Store Review Guidelines, the Google Play Store's Developer Program Policy is generally less restrictive than Apple's Guidelines. For example, Apple's App Store Review Guidelines require that apps should not encourage a user to actively restart their device, or to disable device security features—and Apple App Review checks for this. Google, in comparison, has policies limiting deceptive device setting changes, but does not include requirements relating to preserving on-device security settings. Apple's Guidelines also require apps to use only certain background services (VoIP, audio playback, location, task completion, among others) for their intended purposes. Google's policy does not, and thus even its human reviewers may not review for a Tic-Tac-Toe app that conducts continuous recording through background operations. Google's

policy also does not restrict the use for call and SMS-centric apps for user data collection or spam, unlike Apple's Guidelines. This guideline can have significant consequences for a potential user data breach or malicious blocking of legitimate calls and messages to a user—but would not be enforced if it does not exist.

60. Windows similarly demonstrates the value of app review. Windows has three main issues not present on iOS that hurt its overall security posture of the platform. First, a sizeable portion of Windows computers do not have hardware-backed cryptographic modules and thus Windows OS cannot use these mechanisms for secure key storage and disk encryption across large swaths of its user base. Second, Windows allows for installation of device drivers to allow the operating system to interface with a wide variety of hardware. Malicious or vulnerable device drivers can be used to subvert sandboxing and also to perform other malicious behavior with elevated privileges. Third, Windows supports the installation of software applications from untrusted sources. This has resulted in many malware attacks. In a common scenario, a user receives a malicious email attachment or file download. They execute it and ignore warnings from User Account Control ("UAC"). The user's computer is then infected with malware.

61. Indeed, in the Windows Vista operating system, it became common that users would arbitrarily run malicious programs with administrator privileges using UAC. Microsoft has recognized and warned users about these security risks. But iOS, in contrast to Microsoft, can do more than warn users that using administrative credentials to run an unknown program could render a computer vulnerable to attack. App Review specifically checks for and will reject apps that maliciously requests elevated privileges.

3. The Enterprise and Ad Hoc Distribution Programs Do Not Demonstrate that App Review Is Not Needed

62. Apple provides two distribution options through which apps may not be reviewed by Apple's App Review—the Developer Enterprise program and the Ad Hoc program. Dr. Mickens points to these scenarios as acknowledgement by Apple that App Review is not necessary for security because iOS on-device mechanisms are sufficient to keep users safe. I disagree for several reasons.

63. First, Dr. Mickens's argument ignores the most important aspect of the Enterprise Program: it is intended for use only for company-specific apps. As the name implies, the Enterprise program allows a business enterprise to distribute apps to the company's employees. The fact that the apps are created by an employer, and distributed to employees (typically for free), creates a specific security context that does not exist when third parties are providing apps to strangers (sometimes for money) with whom they have had no prior or existing relationship. Far from proving Dr. Mickens's point that the downloading of an app can be "decoupled" from the verification of the signature on an app, the Enterprise Program merely demonstrates that when there is a relationship such that an employee trusts his or her employer, Apple permits apps from that employer to bypass App Review.

64. This similarly applies in Ad Hoc distribution, which allows a developer to test an app on up to 100 devices. This program allows a developer to test an app on different devices (e.g., iPad Air, iPhone X, and iPhone 12) and on different versions of Apple's iOS operating system to

ensure compatibility. Before apps can run via Ad hoc distribution, their developer must select a valid provisioning profile and compile the app through Xcode. The provisioning profile includes a development certificate used to sign the app. Similarly, to run an in-development app on a developer's devices, the app needs to run on the developer's device with a provisioning profile downloaded through the developer's Apple Developer account, which also includes a development certificate used for code signing.

65. In short, the distribution scales in both circumstances are extremely limited. Enterprise apps are intended for distribution only to users affiliated with their enterprise, and Ad hoc distribution is limited to up to 100 devices that must be specifically identified and registered.

66. Second, despite the limited distribution and the different security context in which these programs operate, there have been several well-known problematic apps distributed through non-reviewed channels, including malware by eSurv and Hacking Team. There are entities that have been revealed as attempting to deliberately utilize the Enterprise program in a manner that would violate Apple's App Store Review Guidelines.

67. Epic is one such entity. It apparently explored the possibility of using the Enterprise program in a manner that certain Epic employees flagged was contrary to Apple's terms and conditions. Specifically, Epic explored using Apple's Enterprise certificates in order to bypass the App Store review process so that Epic could more conveniently distribute its apps (essentially via sideloading). This appeared to be financially motivated, as Epic was "looking at ways to reduce the 30% cut that Apple take[s]." DX-4066.002. Epic not only knew that "using an Enterprise account for external distribution like this [was] firmly against Apple's T&C [terms and conditions]," DX-4066.002, it was also aware that "[c]ertain malware in the past has been able to do this [to bypass app review]." DX-4616.002.

68. Notably, the breaches identified above occurred when the distribution was *not* between an employer to employer, nor from an app developer to a small group of testers. Instead, they occurred when developers attempted to distribute and obtain apps outside of the App Review process on a broader basis. In other words, they occurred when developers attempted to use the Enterprise Program to bypass App Review for broad distribution.

69. In addition, even if developers are well-intentioned, if certain quality checks are not performed because the app has not undergone App Review, broken or unintended functionality can result.

4. macOS Does Not Prove that App Review Is Not Needed

70. Similar to his argument with respect to the Enterprise Program, Dr. Mickens also argues that the ways in which Apple permits app distribution on macOS computers means that App Review is not necessary for meeting Apple's safety standards. I disagree with this argument as well.

71. As I mentioned earlier, the threat model is critical for assessing security for a computing system. iOS, quite simply, faces an extraordinary threat model that is different from—and poses a greater spectrum of risks than—macOS. For one thing, iOS devices contain highly sensitive

personal information—often more sensitive than that stored on a computer. iOS devices, unlike macOS devices, have sensor hardware—such as GPS units and accelerometers—that track their users' location and movement patterns and generate data about their users' current physical environment. iOS devices holding this sensitive data, along with financial data, are smaller than macOS devices and—with their microphones and cameras—are more likely than macOS devices to be with their users at all times. And for iOS devices, an unstable app that causes an iPhone to crash could have devastating consequences; picture, for example, an app that causes your iPhone to crash and be unable to make phone calls when you get a flat tire in the middle of the night. Heightened security systems—and particularly one that includes App Review's review for entitlements, hidden features, requests to access sensitive hardware that are unconnected to the app's purpose, and other threats that could cause an iPhone to crash, among other things—are thus reasonable and necessitated for iOS in a way that they are not for macOS.

72. In the opposite direction, macOS users may expect and require greater access privileges than iOS users. Historically, computer users have held a higher level of privilege in order to perform system/network administration tasks, virtualization, and software development (including for software that will interact with peripherals such as USB devices). To connect a printer to a computer in order to print a term paper or a novel written on that computer, for example, a user typically requires administrative privileges in order to download and install the drivers for a printer. Regardless of whether macOS and iOS share the same kernel, they do not share the same threat model—and that threat model is critical to evaluating whether App Review is necessary for security.

73. I also note that even with respect to macOS, Dr. Mickens acknowledges that one of the app distribution models entails app review. For others, Dr. Mickens points to anti-malware scanning as contributing to the safety of macOS. macOS devices, however, are better positioned to conduct on-device anti-malware scanning than iOS devices. Anti-malware technologies like macOS's XProtect usually contain a real-time scanner, which continually monitors system activities for the presence of malware, and an on-demand scanner. A hook to the operating system alerts the real-time scanner when a file is executed, allowing the scanner to check a file for malware signatures or behaviors. Anti-malware scanners also contain an on-demand scanner, which could be run by the device user at a specified time or interval to check an arbitrary storage location for malware. The arbitrary location may include certain files, folders, or the contents of an entire hard drive.

74. Anti-malware software is able to operate on macOS because macOS generally provides its users with the elevated privileges needed to perform malware scanning. In iOS, those privileges are limited for the reasons explained above and for reasons that Dr. Mickens argues are necessary for providing security on iOS devices—the sandbox compliance that Dr. Mickens identifies as one of the three security properties are entirely enforced by an OS and important to security. In other words, the iOS sandboxing protections that Dr. Mickens identifies as important would prevent anti-malware from operating on apps distributed by third-party app stores. It is for these reasons that Apple currently relies on a preemptive automated scanning process during the App Review process in order to detect whether iOS apps are harmful before they become available for distribution through the App Store. Apple also continues to scan apps that have already been uploaded to the App Store and will remove them if malware is detected.

Apple has a number of tools in place to detect malware on existing apps, that it runs at periodic intervals to capture content at different times.

75. I also should note that, even if anti-malware scanning could occur in iOS, it could be less effective against the types of threats that are prevalent on mobile devices. In an industry study of threats to mobile devices, adware was identified as the most prevalent threat to mobile devices, at 48.02%, and riskware the second most prevalent, at 20.14%. Riskware is defined as legitimate programs that pose potential risks due to security vulnerability, software incompatibility, or legal violations, where malicious actors can take advantage of these programs to access and steal sensitive data or admin-level processes. By contrast, and for context, adware and riskware only make up 7.7% and 3.8% of portable executable threats on the Windows operating system. Even if current anti-malware would hypothetically be applied to iOS, the efficacy could not be determined.

76. The problems that would arise if iOS adopted the "macOS app distribution models" that Dr. Mickens identifies can be previewed by examination of cases of jailbroken iOS devices. Jailbroken iOS devices, like Dr. Mickens's "macOS app distribution models," allow for the download of apps outside the App Store. Jailbreaking refers to a process that modifies Apple's iOS operating system to enable the installation of unauthorized software, including applications from other interfaces, that are not approved by an app review process (like sideloading). It has been well-documented, however, that jailbroken iOS devices suffer from more malware than non-jailbroken iOS devices. Malware can be distributed via unreviewed apps and, moreover, can use elevated privilege levels possessed in light of their lack of review to perform malicious activity. Dr. Mickens's "macOS app distribution model" proposal would, however, move iOS towards a "universal" jailbroken iOS phone and the greater exposure to threats that this would entail.

C. The Introduction of Alternative App Stores Would Decrease the Security, Safety, Reliability and Trustworthiness of the iOS Platform

77. Dr. Lee suggests that third-party app stores could achieve the same security goal as the App Store, and Dr. Mickens suggests that, in the event of third-party app stores, iOS users would not see diminished security. I disagree with that conclusion.

78. The introduction of third-party app stores for iOS would decrease iOS security, safety, and trustworthiness, as evidenced by the cases of Google and statistics indicating that third-party app stores host 99.9% of discovered mobile malware. DX-4956.004. Irrespective of whether they would be able to or intend to achieve the same security goals, the reality is that they could not. Moreover, there is no guarantee that all, or even most, third-party app stores would commit to upholding user security and privacy and intend to achieve such security goals, particularly if those standards come at the expense of efficiency and revenue.

79. In fact, I understand that Mr. Sweeney would not anticipate third-party stores to adhere to security standards; I understand that he believes that app stores can make decisions about the quality and other attributes of the apps they will distribute. In other words, Mr. Sweeney does not consider it to be a problem that third-party app stores give up security controls for time and cost

efficiency, as long as the third-party app stores think the surrendered security controls are not necessary, without thinking about the security implication behind this situation.

1. Third-Party App Stores May Not Have the Incentives to Provide as Secure an App Store Experience as Apple

80. Epic's experts suggest that even if app distribution were opened up, the security of the iOS platform would remain uncompromised because at least some third-party app stores theoretically could engage in the app review process as Apple is currently doing.

81. To begin with, neither of Epic's experts opine that *all* third-party stores would even attempt to engage in the app review process that Apple currently undertakes. They only speculate that some of those stores might attempt to emulate Apple's processes.

82. Outside of the iOS platform, we know that there currently are distribution sites that specifically traffic in the types of apps—such as pirated apps—that Apple prohibits. ~~If permitted to operate and distribute iOS apps, these stores would have no incentive, and are unlikely to attempt, to duplicate Apple's app review efforts. Even third parties that don't explicitly traffic in illegal and malicious content are unlikely to match Apple's App Review efforts for several reasons.~~

83. First, many third-party stores, including those that target niche markets, lack the resources or commitment to review apps in the way that Apple does. Apple has outpaced its competitors in protecting user privacy. As noted above, Apple's process is a comprehensive one that includes not only human reviewers, but teams of dedicated engineers who create tools, including machine-learning tools, specifically to help Apple combat efforts to subvert the app review process.

84. ~~Second, the incentives of third-party stores may drive them to deliberately adopt a standard lower than Apple's~~. For example, certain large companies are heavily dependent on ad revenue, which in turn, is heavily dependent on the ability of an app to track user behavior. Other companies may choose to maintain different standards. For example, Apple's App Store Review Guidelines reject apps that alter or disable standard device inputs like device volume buttons, but the Google Play Store's Developer Program Policy does not have a similar requirement. Returning to the Tic-Tac-Toe app example, if it also included an instruction to users to reconfigure their devices to raise the volume on the microphone to enhance listening sensitivity, Google might allow that app for distribution via the Google Play Store where Apple might not. As mentioned earlier, Google similarly does not have guidelines pertinent to privacy protection such as the Apple App Store Review Guidelines that limit background activity to specific functions and restrict the calling of and collection of SMS data. Another example is the GOG app store, which operates on PCs and has a business model of restoring old, unworkable, or unoptimized games. Because GOG's purpose is to make unworkable games work again, not to provide secure apps, it likely prioritizes security less than the App Store.

85. Third, even if a third-party store has the best of intents, practical consequences such as meeting a deadline to release a product may result in them "bypassing" certain review guidelines on a one-off basis. For example, the videogame Cyberpunk 2077 recently was released with a

considerable number of bugs and glitches. Sony had to pull Cyberpunk 2077 from the PlayStation Store and offer users full refunds because the game was unplayable on certain PlayStation consoles. Cyberpunk 2077 is an example of a game that was released at full price before it had been sufficiently debugged, and it demonstrates how developers may prioritize profit over reliability. I raise this example not to impugn this specific product, but to suggest that when companies are faced with deadlines and marketing campaigns, those pressures may be at odds with even well-intentioned developers and app review guidelines.

86. Even Epic's own CEO and Vice President of the Epic Games Store recognize that third-party app stores could hold differing incentives. Steven Allison, Epic's Vice President of the Epic Games Store ("EGS"), will testify that EGS, unlike Steam, would not support certain kinds of content like anti-games, which are offensive and sexual in orientation and will be curated based on standards against porn and hate. As Mr. Sweeney will testify, Epic curates its own Epic Games Store and recognizes that app stores can present customers with different quality, selection, and policies.

2. iOS Security Would Be Impaired if Even One Third-Party App Store Does Not, or Chooses Not to, Maintain Strong Security Measures

87. In the area of computer security, it is generally understood that "security is only as strong as the weakest link." What this means is that in a fragmented distribution landscape, bad apps need to find only one app store with less than adequate security measures in order to jeopardize overall safety of iOS and infiltrate the iOS ecosystem. If there were nine stores, an attacker could simply submit his app to all nine stores, and as long as one store were to accept the app, it would then become available to the public. The scenario is not limited to intentional attacks. If an app unintentionally contains a bug that causes it to crash, it also would be available to the public as long as one of the stores accepted the app. Third-party app stores thus would increase the attack surface of iOS and weaken its overall security.

The situation becomes more dire when one considers that not all stores will even pretend to care about security. Stores referred to as "rogue app stores" are known to deliberately host and distribute pirated content and apps containing malware and user data theft. In China, Android app stores are known to violate security and privacy regulations, with nearly 35 percent of Android apps secretly stealing user data unrelated to their functionality. These third-party stores either choose not to or are not capable of enforcing security and privacy guidelines like Apple's and the presence of even one such store on iOS could significantly diminish iOS's overall security.

88. The presence of third-party app stores thus has the potential to significantly diminish the overall security of Apple's App Store (and the iOS platform). When Apple discovers malicious apps that have successfully circumvented the App Store review process, it adjusts the review process to prevent such apps from successfully being approved in the future. If Apple discovers apps that have not circumvented the App Store review process per se but that are exhibiting malicious or user-unfriendly behaviors *after* installation, Apple similarly adjusts its processes to prevent this from reoccurring. If Apple discovers new malware on the iOS platform, it can explicitly adjust its custom-written malware scanners to scan apps already on the App Store and to detect such malware in the future. Apple is able to do all of these things because it controls all

aspects of its platform. Drs. Mickens and Lee are not only wrong to opine that Apple's App Store review process adds only marginal security benefits at best, but are also wrong to opine that third-party app stores can provide equivalent security to Apple's app store review process.

89. Furthermore, the fragmentation proposed by Epic's experts would limit Apple's ability to deter or otherwise take action against such attackers. Where Apple's App Store acts as the only way to distribute apps, Apple could freeze or terminate that attacker's account in order to prevent them from any further legitimate distribution of apps and app updates that violate Apple's Guidelines, as well as check for similar issues in other apps. In the world proposed by Epic, iOS would, like Android, no longer have a single "spigot" of app distribution and therefore be less able to prevent the distribution of known malicious apps on iOS.

3. The Presence of Third-Party App Stores Would Weaken the Security Provided by Apple's App Review as well as by Well-Meaning Third Parties

90. The centralization of iOS and App Store distribution not only prevents multiple stores from acting as the "weakest link," but it also strengthens Apple's ability to implement measures to protect iOS security. By contrast, weakened protections can lead to the deterioration of user trust in iOS, which might lead to more severe risk scenarios in which users refuse to apply Apple-recommended security measures such as downloading software updates.

91. Given Apple's centralized iOS app distribution channel, Apple's App Review has transparency over all apps distributed through the App Store, which covers the absolute majority of apps utilized by iOS devices. Apple's App Review process thus has and relies on a catalog of historic review decisions Apple has made with respect to tens of millions of apps, which is used to continuously update Apple's tools and serves as a resource to train and educate Apple's human reviewers. Apple has made numerous choices intended to present a safe, reliable, and trustworthy app experience, including all of these as well as restrictions on the addition and removal of apps that permit users to remove preinstalled apps. Apple also takes the responsibility to eliminate "weakest links" for iOS app security and app distribution to better protect its users, instead of forcing individual users to identify secure, trustworthy app marketplaces on their own, just to protect themselves. Indeed, Epic's experts do not dispute that curation of apps provides additional layers through which security and privacy can be protected. Approving low-quality apps that pose security and trust risks would, for example, degrade iOS users' experience and likely cause a loss of goodwill with respect to users and, ultimately, the attractiveness of Apple's app experience to developers.

92. Apple's catalog of review information would see reduced effectiveness if third-party app stores were allowed to approve and distribute their apps on iOS. I mentioned earlier the "Update your Adobe Flash Player" plugin scam, where multiple websites would display a pop-up intended to get a user to click on and install adware or other types of malware. In the app context, where all apps are reviewed by Apple for distribution through the App Store, Apple would be able to catalog, detect, and block each instance of apps containing the website links containing the malware plugin. Where, however, third-party app stores also could distribute their apps on iOS, the likelihood increases that one or more of those other app stores might not block an app pointing to an "Update your Adobe Flash Player" malware plugin, perhaps because

that app store had not been able to catalog all of the website links associated with the malware plugin. And this would be a problem not just for malware websites, but also new types of malware, new trends in malicious apps, new methods of social engineering attacks, and other red flag information might not make it into the databases for Apple and all other third-party app stores distributing apps on iOS.

93. This could pose problems not just for Apple's App Review, but for all third-party stores endeavoring to enforce security guidelines on iOS. This would effectively render all app review conducted by all of the app stores less useful over time. With multiple third-party app stores, the Apple App Store, and each third-party app store, would see only a subset of all existing data—such as a subset of malware signatures—resulting from the malicious apps that were caught in their respective app review process. By allowing multiple app stores, the app stores all would become less effective as key information becomes decentralized, leaving app stores with fragmented knowledge of how the iOS platform is operating. Whether Apple was able to enforce security standards or not, and even where security breaches occurred because of a third-party app store's ineffective review process, users might attribute those security breaches to the iOS platform, and, by consequence, Apple. This ultimately would risk users' safety and erode the trust of the iOS platform.

94. The "Cuphead" game provides a real-life example where fragmentation permitted an app that otherwise would have been caught during App Review to make it through (temporarily). Cuphead is a game that was available on the PC third-party app store and gaming platform Steam. Developers then created a copycat of Cuphead and submitted it to the App Store with screenshots from the legitimate game and under a name similar to that of the Cuphead developer, StudioMDHR. Apple ultimately pulled the app from the App Store after StudioMDHR reported the app as an imposter to Apple.

4. Users Have Limited Ability to "Choose" between Safe and Unsafe Third-Party Stores

95. Epic's experts seem to opine that even if some app distribution stores will have lower (or no) security standards, that would not degrade iOS security and trustworthiness because individual users can make informed decisions about which stores to shop at, and which apps to download. This assumption is problematic for several reasons.

96. First, the general user population may lack the security-oriented technical understanding—and the incentive to gain such understanding—needed to make accurate decisions regarding security and privacy. For these reasons, social engineering attacks, spyware operating in the background, and cryptojacking—particularly those that circumvent app review channels—have been particularly successful. With social engineering as an example, DX-4956, a report published by cybersecurity company Purplesec in 2020 identified that "98% of cyber-attacks rely on social engineering" and that the total malware infection growth rate has been increasing by hundreds of millions every year (812.67 million infections reported in 2018, a significant increase from 702.06 million reported in 2017). Similarly, 9Game.com is still the largest mobile game market platform in India despite being considered by RiskIQ as the "most dangerous" app store with 61,669 Android apps associated with potential security threats—the *highest* concentration of potentially insecure Android apps. DX-4401.005.

97. Even if some users have a certain degree of technical sophistication, it is sometimes still very hard for them to identify that they are under attack, let along perform attribution. After all, one goal of attackers is to keep the victim from realizing that an attack has occurred; this allows the attacker to maximize the number of victims as well as the "payout" before the attack is discovered and perhaps shut down.

98. Epic's position also relies on the assumption that a user has a realistic choice among multiple app stores. As the PC and Chinese Android marketplaces show, and as Mr. Federighi will testify, this is not a realistic assumption outside of the iOS App Store. Users may not always have control over what software they install, and if the software is not available in the App Store, users may have to go to a less secure app store in order to obtain that software. This will, as I explained above, open up iOS to the "weakest link" and make iOS users less secure.

99. Indeed, if a third-party app store provides exclusive content that is only available on its platform, users might have no choice but to use that store regardless of whether it is secure or reliable. Exclusivity, for example, has been one of Epic's most prominent business strategies. Epic has heavily leveraged content exclusivity by making certain content only available through the Epic Games Store and Mr. Sweeney has confirmed that Epic seeks to negotiate content exclusivity deals that prevent Steam from having the same content that is available in the Epic Games Store.

5. The Case Study of the Android Marketplace in China Demonstrates the Security Problems that Arise From Fragmentation

100. The various concerns I raise here are not merely theoretical. The Android marketplace in China illustrates the real-life consequences of fragmentation of app distribution.

101. As Dr. Evans explains, the Android operating system for mobile phones is created and maintained by Google. Throughout the world, Google operates the Google Play app store through which many developers choose to distribute their Android apps. Apps distributed through the Google Play Store are reviewed by computers as well as, sometimes, humans, in accordance with Google's Developer Program Policy. But developers also have the option of distributing their apps outside of the Google Play store for Android devices.

102. In China, the Google Play Store is banned. And in place of a centralized Google Play Store, a variety of other app distribution stores have popped up instead. The multitude of Android app stores in China has not improved Android security in that country. To the contrary, China faces a very significant and frequent risk of malware arising from the numerous Android app stores that are available to Chinese users—and the multitude of those app stores has facilitated that frequency.

103. As seen in DX-4934, RiskIQ's 2020 Mobile App Threat Landscape Report, the top three stores (Xiaomi, Baidu, and Pconline) where users were most likely to download malware are all from China and heavily used by Chinese users. This has translated to Chinese users facing increasing security risks when obtaining apps from these app stores. As far back as 2013, studies have shown that the fragmentation in China's Android market has resulted in "nearly 35 percent of the Android apps . . . secretly stealing user data unrelated to the app's functionality." DX-

4555. Just within the first month of 2021, 157 apps on China's Android app stores were discovered by China's Ministry of Industry and Information Technology to be violating security and privacy regulations; these included widely-used apps from large corporations, such as apps developed by Tencent.

104. The proliferation of malicious apps in China's Android market is largely attributed to looser security standards that accompany the multitude of app stores distributing apps. In a 2018 study analyzing over 6 million Android apps obtained from 16 Chinese Android app stores and Google Play, the Chinese Android app market was found to have a higher prevalence of fake, cloned, and malicious apps in Chinese stores than in Google Play, possibly due to market operators indulgently oversighting copyright and security checks over the apps. As found in a 2020 study, various Android apps in China require more default permissions than their iOS counterparts and therefore entail fewer function-specific authorization requests than on iOS devices. The default permissions in Android grant access to certain types of data by default when users install and use the app. In this case, Chinese users not only face looser security standards, they are also left at their discretion to make cybersecurity-related decisions such as whether to change authorization permissions or privacy settings. As I discussed above, not forcing users to make those types of decisions facilitates a much safer mobile app distribution ecosystem.

6. Implementing Epic's Experts' Proposals Would Entail Changing iOS in a Manner That Could Open New Threats and Have Negative Security Impacts

105. Apple specifically designed its iOS software and hardware to prevent the download and installation of apps outside the App Store. Changing iOS to permit third-party app stores as Drs. Lee and Mickens appear to suggest, however, could create new threats and negative security impacts.

a) On-Device Malware Scanning Would Require Weakening of the Sandbox and Would Not Necessarily Provide Sufficient Protection

106. As I noted earlier, Dr. Mickens argues that the introduction of third-party stores on iOS would not hinder security because Apple could apply anti-malware protection to scan apps on iOS devices. However, the use of anti-malware scanning would require changing, and therefore weakening, Apple's current sandboxing.

107. The anti-malware apps that Dr. Mickens proposes would need operating system hooks to perform real-time monitoring, and file access inside other apps' sandboxes to perform on-demand scanning. Apps performing these activities would require high-level system privileges, and they would break through iOS sandbox protections with every scan activity. These scenarios lead to heightened security risks. These scenarios also may lead to detrimental impairment to device usability. Constantly running anti-malware scans and updates negatively impacts user experience, since these activities would significantly drain a device's battery and reduce overall performance.

b) Sharing Entitlements and Apple's Private APIs Will Create Vulnerabilities and Potential Instabilities

108. Drs. Lee and Mickens also suggest, or otherwise appear to assume, that third-party app stores and/or app developers would be provided with a list of Apple's private APIs and entitlement management ability. Both of these suggestions also present security concerns, particularly if used by third-party app developers outside established security review procedures and standards.

109. Apple's App Store Review Guidelines currently forbid the use of Apple's private APIs, which might be used to perform unauthorized activities or to extort private information; they might also change any time and break app stability. As Dr. Lee acknowledged in his expert report, private APIs can be used, for example, to allow attackers to circumvent iOS sandbox or obtain private data without permission. Apple's private API detection during App Review is backed by a complete list of private APIs that it internally collects and manages. This is an example where Apple's knowledge base distinguishes itself; Apple has developed automated processes to detect whether the APIs called by an app are private APIs or some of the thousands of APIs on the iOS platform. Apple's computer tools here operate accurately and efficiently (and can outperform humans in this type of review). Apple's control of private APIs is a part of Apple's commitment to user privacy and security; restricting third-party use of Apple's private APIs helps ensure that apps cannot interfere with the core functions and stability of iOS.

110. Apple also manages the entitlements granted to third-party apps in connection with protecting against potential security, privacy, and reliability threats. Drs. Lee and Mickens have not, however, addressed the management of entitlements and signing in their proposed multi-app store scenario, including who would be responsible for evaluating requested entitlements or checking signing of apps for third-party app stores.

111. Currently, when developers want to test their app, Apple provides them with a provisioning profile, which is a type of system profile used to launch one or more apps on devices and use certain services. Entitlements are granted to apps when a user is given this provisioning profile. According to Apple's current process, app developers must request special entitlements from Apple, who will review an app's use case to ensure privacy policies are followed appropriately and in accordance with the legitimate purpose of that app.

112. However, permitting third-party stores could mean that developers deploying apps for third-party app stores would not need Apple-provided provisioning profiles and therefore grant themselves their own entitlements (as well as first-party entitlements, which are entitlements that can only be used by Apple in the current environment). By consequence, apps distributed through third-party app stores could easily be granted elevated privileges that allow apps to bypass certain on-device security.

113. Dr. Mickens states that a majority of security measures enforced during app review could be implemented using on-device security, but if apps can easily circumvent these protections because they are granted (or can grant themselves) certain entitlements, then these on-device protections would be largely irrelevant. This furthers my opinion that app review is necessary, and that allowing third-party app stores onto iOS could present serious security concerns.

114. For example, when Epic distributed *Fortnite* to Samsung devices using its own third-party downloader, the game was installed silently via a private Samsung Galaxy Apps API. A silent download implies that users are not given any prompts to confirm the permissions that the game requests. This signifies the importance of controlling entitlements. If other apps followed in Epic's footsteps, they could easily access privileged functionality without alerting the user. In the absence of Apple as an arbiter evaluating and granting entitlements in connection with efforts to guarantee a level of security and privacy on par with Apple's standards, the lack of restriction on entitlements for apps distributed through third-party app stores could undermine the security, privacy, and reliability of the entirety of the iOS ecosystem.

115. Moreover, the consequences of granting entitlements and signing without regard for the potential risks created by those processes can be very substantial as it would result in a less secure app landscape where users are free to acquire apps from arbitrary third-party origins. Previously, I explained that such a process of downloading apps from arbitrary sources and insecure third-party app stores contributes to the fact that Android is less secure than iOS. Downloading from external sources on Android allows for the direct distribution of unreviewed apps that are potentially malicious, and there is no way for users to verify whether these apps meet a certain security standard. At the same time, there is no single "spigot" through which Android OS companies or OEMs can control or limit the dissemination of malicious apps once they are detected, which is opposite of what Apple is able to do on iOS. Apple can remove the app from the App Store and revoke the developer's certificate, preventing them from uploading new apps or updates signed by the revoked certificate to the App Store.

116. If Apple is not permitted to itself evaluate entitlements and signing of apps to be released on the iOS platform, Apple would be forced to rely upon third-party certificates for app verification. This could encompass, for example, needing to allow third parties to install root certificates on iOS for app verification. Furthermore, it exposes Apple and its users to potential propagation of malicious apps on iOS using a stamp of a third-party that is compromised, has lost control of their private key, maintains an insecure app review process, or even has a rogue employee. This could critically and irreversibly hurt the overall security of the iOS platform.

117. Again, an example with respect to Epic's activity on Android devices—which lack entitlement and verification control—is instructive. Epic launched *Fortnite Installer* on Android devices via third-party stores and sideloading in August 2018. A Man-in-The Disk (MiTD) vulnerability—which is an attack that allows an intruder to intercept and potentially alter data that moves between Android external storage and an installed mobile app—was discovered in the installer soon after the release. The MiTD vulnerability allowed an attacker to hijack the app installation process and install arbitrary apps in the background of the user device. Those arbitrary apps installed through this vulnerability could have granted themselves full access permissions without the user's knowledge. In this instance, Epic had little to no control of *Fortnite Installer* being continuously downloaded, since the installer could be uploaded to any third-party app store by any user that had already downloaded the APK, and Epic could not control any malicious exploits that had been introduced into the devices that downloaded *Fortnite* using the installer.

c) Epic's Proposals Have Additional Significant Negative Security Impacts that They Have Not Fully Assessed

118. Even assuming that third parties would be able to replicate Apple's App Review process, there is no guarantee that they would seek to implement comparable security measures. It is notable that Epic and its Epic's experts failed to set out a framework for the relationship between Apple and any third-party store. Thus, it is unclear what they envision third-party app stores would—in practice—be permitted and entitled to do. The current state of the industry, however, and the examples of the Chinese Android app marketplace and Google's Google Play Store review process, suggests that third parties would be unable to, or not inclined to, implement the same level of security, privacy, and reliability review as that of Apple. The introduction of third-party app stores thus would be likely to create additional vulnerabilities and security threats for iOS.

119. Epic's experts suggested that Apple should provide security guarantees and help third-party app stores, if they were to exist, achieve the same security goals as the App Store. Epic's experts assume, however, that Apple will continue its security and trustworthiness efforts at the same pace and to share the fruits of those efforts with all third-party stores (apparently without, however, those third-party stores sharing in the cost of vetting apps, monitoring the iOS ecosystem, connecting with third parties, and providing support to developers and users). If, however, Apple could not set security guidelines for or otherwise prohibit the distribution of unsafe, illegal, and/or malicious apps, security, privacy and trustworthiness could be significantly degraded. This could occur, for example, if Apple could not prohibit a third-party app store from distributing a pirated and fake version of well-known apps that seeks to obtain private and sensitive user information, such as users' credit card information. Similarly, if third-party developers and app stores were to discover and exploit a security vulnerability, I would be concerned if Apple were not able to update its iOS platform to address that security vulnerability, regardless of whether an update results in those apps no longer being operable on iOS.

120. Dr. Mickens focuses on macOS security mechanisms such as the "warning dialog" that macOS will display when a user tries to install an unsigned, unnotarized app, and the fact that the user can override that warning and install the app. But it is unclear whether Apple actually could issue such warnings in a hypothetical world where Apple is not permitted to take actions that have the "effect of impeding or deterring competition among app distributors (including competition between third-party app distributors and the App Store)." The absence of such warnings, however, would have significant negative effects; although I believe that such warnings are not sufficient to protect users, there may be few other ways for unsuspecting users to differentiate the level of security that Apple offers from what other app stores offer. The open question of whether Apple could provide security measures or have involvement in third-party app stores thus presents another security risk not considered by Dr. Mickens.

121. Epics' experts proposals could have additional negative security impacts. As I explained earlier, third parties lack Apple's internal feedback loop available for Apple's App reviewers. App reviewers are able to make suggestions to the App Store Review Guideline, and to escalate app review findings and issues to other Apple teams handling policy, processes, and products, both through internal Apple channels. As Mr. Kosmynka will testify, internal communications

between app reviewers and iOS engineers have led to iOS updates with security and privacy advancements based on new issues identified during app review.

122. However, third-party reviewers would also be incapable of acquiring and utilizing Apple's open channels of communication available to Apple reviewers. Even if some feedback loops can be established between third-party reviewers and Apple, it would be hardly as efficient as Apple's internal communication channels, which would lead to amplified response time for incident response. In addition, Epic and its experts are silent on whether each app store should establish a one-on-one channel with Apple, or Apple could just establish a communication platform that every store could participate. They are further silent on who would be in charge of building and maintaining such communication channels.

123. There is also no guarantee that third-party app stores would provide feedback to Apple on their security findings. There is also no guarantee that, if they are willing to share, they will share all necessary information in a timely manner. It has to be noted that there is competition among app distributors (including competition between third-party app distributors and the App Store). Such competition might inhibit certain parties' intention to share information.

124. Potentially differing levels of security across app stores thus raise questions as to who will scrutinize third-party app stores, Apple's ability to ensure the safety of its iOS platform, and the extent to which security, privacy, and reliability on iOS would be negatively impacted by permitting third-party app stores on iOS. On Android, which permits sideloading, there can be no effective scrutiny, and Android thus has faced third-party app stores acting as malicious app vectors as a result. Epic's proposed scenario does not address or try to quantify the impact on security, how third-party app stores would be held accountable if they get caught "cheating" and not following platform rules; or if they become a significant vector of malware for the iOS platform? Similarly, Epic's proposed scenario does not address a situation where Epic, for example, could take actions through app stores on iOS that hurt Apple's users, but Epic would be indifferent because it could collect revenue by offering the same products elsewhere. If Apple is prohibited from creating and enforcing security policies, Apple could be constricted in what steps it can take to provide security measures or otherwise ensure that app stores meet security guidelines. Apple would be unable to leverage the experience and knowledge with its own technology and standards in seeking to ensure that third parties meet those standards. And what recourse would Apple have if third-party app stores tarnish the platform's reputation or place its users at risk or directly in harm's way? Apple could have to incur even more costs in an effort to monitor its ecosystem and provide support to users who face those risks (and potentially attribute some of that responsibility to Apple as the iOS platform provider). Epic and its experts fail to realize that it will be a negative-sum game for iOS security if certain third-party app stores give up security controls and choose not to commit to Apple's security and privacy objectives. Where third-party app stores consider deviating from the high standards of security and trust that Apple has set, the protective mechanisms that Apple has put in place would have diminished effect and Apple, its developers, and its users would face additional costs and risks. This will compromise the integrity of the iOS platform as well as ultimately put app users in harm's way.

D. Diversifying In-App Purchase Channels Could Inhibit Apple's Anti-Fraud Abilities

125. IAP is a single, secure, and efficient solution that consumers have learned to trust. The IAP functionality provided by Apple aids in protecting security and privacy in the iOS platform, including through sophisticated fraud detection. These benefits are shared by consumers, developers, and Apple itself.

126. Allowing third-party payment systems, similar to allowing third-party app distribution mechanisms, could lead to less secure payment mechanisms and differing security standards that would facilitate bad acts. ~~Apple has developed significant and extensive security protections, including the use of cryptographically signed attestations, tamper-resistant Hardware Security Modules ("HSMs"), and other mechanisms for safeguarding user data. IAP protects the privacy and security of iOS users by withholding their private information from developers as well as Apple employees. Users' different payment methods and payment details are stored in the tamper resistant HSM on a server, so even Apple employees do not have access to them. Thus, when a customer wants to make an in-app purchase, once the user is authenticated, the transaction can happen seamlessly and securely. Apple also provides cryptographically signed attestations that tie an application's state to a particular device. This allows a developer to have the assurance that customers are not cheating their application with multiple devices that are shared by different users. This proprietary functionality enables IAP to benefit from the ability to utilize such features as the on-device store kit, which can be used to verify whether a receipt for a purchase is authentic.~~

127. Third parties, however, may be unable to, or choose not to, use Apple's proprietary on-device cryptographic hardware, hardware-based attestations, or IAP APIs, which Apple maintains confidentially in order to protect PII of Apple's customers. I also have not seen any commitments, by Epic or Epic's experts, that third parties should be required to utilize reputable payment handlers as third-party payment mechanisms. Thus, where multiple parties are processing payments of digital goods in apps, a fraudster could choose one payment method that is easier to exploit, or bounce between payment methods and payment processors to avoid detection. Breach of a third-party payment system would potentially expose private data, including financial information and PII, to attackers.

128. Allowing third-party payment systems also would curtail Apple's ability to monitor and detect fraud and abuse. Use of Apple's IAP functionality centralizes the purchase of digital goods and services in apps with IAP, safeguards user data, and maintains visibility into the entire payment process. For example, Apple checks that a developer server has confirmed receipt and that the customer has in fact purchased the content before it is delivered to the customer. This maintains the integrity and traceability of the transaction and confirms developer's receipt of transaction, and the delivery of digital goods to appropriate customers. It also enables Apple's fraud algorithms to process as much information as possible across all the transactions. Apple uses this deep learning system to determine whether an account has been compromised. These types of learning techniques are more accurate when more data points are available. IAP fraud protection is enhanced by the very fact that it operates in a centralized system for the entire iOS ecosystem. The balkanization of in-app payment processing systems thus would limit the amount of data that Apple can aggregate and analyze overall—and consequently, the fraud

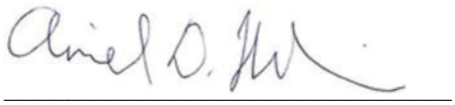
algorithms that rely upon this data. Apple's fraud detection could therefore become less effective if only receiving a skewed subset of all IAP data.

129. In fact, a case study from the Epic Games Store demonstrates the increased risk of fraud that can arise when not using Apple's secure IAP functionality. When Epic Games Store implemented an integration with Ubisoft's Uplay, a 70% fraud rate was observed in transactions within the first 48 hours. Mr. Sweeney indicated that "[s]ophisticated hackers were… selling the linked Uplay accounts faster than we were disabling linked Uplay purchases for fraud." DX-3536.001. Epic ultimately had to disable purchasing of Ubisoft games because it could not handle these fraud transactions.

IV. Oath

I declare under penalty of perjury under the laws of the United States that the foregoing is true and correct.

Respectfully submitted.



Aviel D. Rubin, Ph.D.

April 23, 2021

Word count: 16,253